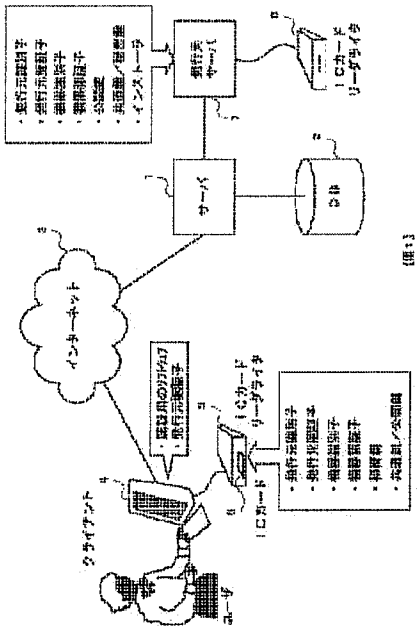
Data updating method and data updating system

Publication number: JP2003337923 (A)
Publication date: 2003-11-28
Inventor(s):
Applicant(s):
Classification:
- international: ***G06F12/14; G06F21/00; G06F21/20; G06F21/24; G06K17/00; G07F7/10;*** **G06F12/14; G06F21/00; G06F21/20; G06K17/00; G07F7/10;** (IPC1-7): G06K17/00; G06F12/14; G06F15/00
- European: G06F21/00N5A; G07F7/10D4E2
Application number: JP20020144486 20020520
Priority number(s): JP20020144486 20020520

Also published as:
JP3754004 (B2)
EP1365307 (A2)
EP1365307 (A3)
EP1365307 (B1)
US2003217270 (A1)

Abstract of **JP 2003337923 (A)**

PROBLEM TO BE SOLVED: To provide a method and a system for data update which can update data of an IC card through a network without mistaking the IC card to be updated.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－337923
（P2003－337923A）
(43)公開日　平成15年11月28日(2003.11.28)

(51)Int.Cl.[7]	識別記号	FI		テーマコード(参考)
G06K 17/00		G06K 17/00	D	5B017
G06F 12/14	320	G06F 12/14	320F	5B058
15/00	330	15/00	330G	5B085

審査請求　有　　請求項の数14　ＯＬ　（全 10 頁）

(21)出願番号　特願2002－144486(P2002－144486)

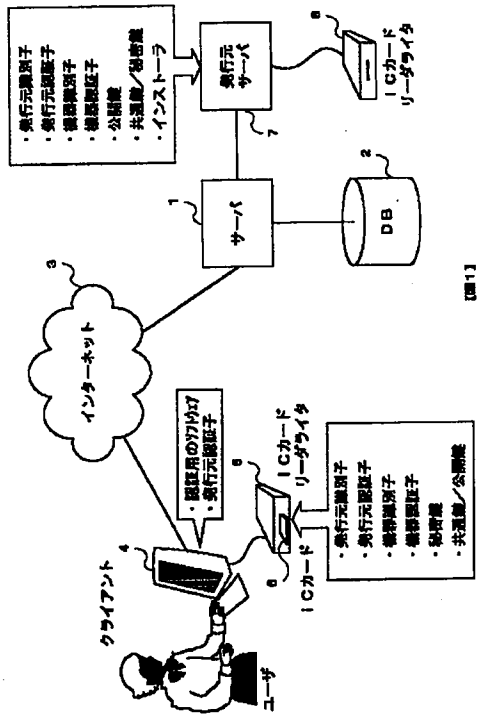
(22)出願日　平成14年５月20日(2002.5.20)

(71)出願人　597115082
システムニーズ株式会社
東京都港区芝２丁目３番３号
(72)発明者　中山　恵介
東京都港区芝大門２－12－９　システムニーズ株式会社内
(74)代理人　100093104
弁理士　船津　暢宏　（外１名）

Ｆターム(参考)　5B017 AA02 BA05 CA14
5B058 CA27 KA08 KA11 KA35
5B085 AE12

(54)【発明の名称】　データ更新方法及びデータ更新システム

(57)【要約】
【課題】　本発明は、更新対象のＩＣカードを間違えることなくネットワークを介してＩＣカードのデータを更新できるデータ更新方法及びデータ更新システムを提供する。
【解決手段】　発行元クライアント認証、本人認証、発行元サーバ認証、機器認証の各認証が為されると、機器認証に用いる公開鍵で暗号化された更新データをサーバ１がクライアント４に送信すると、クライアント４が当該暗号化された更新データをＩＣカード６に出力し、ＩＣカード６は機器認証に用いる秘密鍵で更新データを復号化し、その復号化した更新データでＩＣカード６内の書き替えを行うデータ更新方法及びデータ更新システムである。



1

【特許請求の範囲】

【請求項１】　機器認証に用いる秘密鍵を記憶する装置についてサーバが機器認証を行い、当該秘密鍵に対応する公開鍵を用いて暗号化された更新データを前記装置が接続するクライアントに送信し、当該クライアントが前記装置に当該更新データを入力し、前記装置が前記秘密鍵で前記更新データを復号し、復号した更新データで装置内のデータ更新を行うことを特徴とするデータ更新方法。

【請求項２】　機器認証に用いる秘密鍵を記憶する装置についてサーバが機器認証を行い、当該秘密鍵に対応する公開鍵を用いて暗号化された更新データを前記装置が接続するクライアントに送信し、当該クライアントが前記装置に当該更新データを入力し、前記装置が前記更新データを記憶し、更新データが利用される毎に前記秘密鍵で前記更新データを復号し、復号した更新データを利用のために提供することを特徴とするデータ更新方法。

【請求項３】　機器認証に用いる秘密鍵を記憶する装置には、共通鍵又は公開鍵で暗号化された発行元認証子が記憶され、サーバは前記共通鍵又は前記公開鍵に対応する秘密鍵を用い、前記装置からの暗号化された発行元機器認証子を当該共通鍵又は当該秘密鍵で復号して発行元識別子を取得し、当該取得した発行元識別子と記憶する発行元識別子とを比較照合して発行元サーバ認証を行うことを特徴とする請求項１又は２記載のデータ更新方法。

【請求項４】　クライアントは、発行元から発行元認証子を取得し、発行元サーバ認証の前に、装置から読み込んだ発行元認証子と前記取得した発行元認証子とを比較照合して発行元クライアント認証を行うことを特徴とする請求項３記載のデータ更新方法。

【請求項５】　装置は、本人認証の機能を備え、発行元クライアント認証、本人認証、発行元サーバ認証、機器認証を行い、データ更新を行うことを特徴とする請求項４記載のデータ更新方法。

【請求項６】　機器認証に用いる秘密鍵を記憶する装置と、

機器認証が為されると、前記秘密鍵に対応する公開鍵で暗号化された更新データを機器認証が為された装置宛に送信するサーバと、

前記送信された暗号化された更新データを受信して前記装置に出力するクライアントとを備え、

前記装置は、前記クライアントから入力された暗号化された更新データを前記秘密鍵で復号し、当該復号した更新データで装置内のデータ更新を行う装置であることを特徴とするデータ更新システム。

【請求項７】　機器認証に用いる秘密鍵を記憶する装置と、

機器認証が為されると、前記秘密鍵に対応する公開鍵で暗号化された更新データを機器認証が為された装置宛に送信するサーバと、

前記送信された暗号化された更新データを受信して前記装置に出力するクライアントとを備え、

前記装置は、前記クライアントから入力された暗号化された更新データを記憶し、更新データが利用される毎に前記秘密鍵で前記更新データを復号し、当該復号した更新データを利用のために提供する装置であることを特徴とするデータ更新システム。

【請求項８】　サーバは、乱数を発生させ、当該乱数をクライアントに送信すると共に、前記クライアントから受信した暗号化された乱数を受信した機器識別子に対応する公開鍵で復号し、当該復号された乱数と前記発生させた乱数を比較照合して機器認証を行うサーバであり、

前記クライアントは、前記サーバから受信した乱数を装置に出力すると共に、前記装置から入力された暗号化された乱数及び機器識別子を前記サーバに送信するクライアントであり、

前記装置は、前記クライアントから入力された乱数を前記秘密鍵で暗号化し、記憶する機器識別子と前記暗号化された乱数を前記クライアントに出力する装置であることを特徴とする請求項６又は７記載のデータ更新システム。

【請求項９】　サーバは、乱数と、機器識別子を暗号化するための共通鍵をクライアントに送信し、前記クライアントから受信した暗号化された機器識別子を前記共通鍵で復号し、当該復号された機器識別子に対応する公開鍵で暗号化された乱数を復号し、当該復号された乱数と前記発生させた乱数を比較照合して機器認証を行うサーバであり、

前記クライアントは、前記サーバから受信した乱数及び共通鍵を装置に出力すると共に、前記装置から入力された暗号化された乱数及び暗号化された機器識別子を前記サーバに送信するクライアントであり、

前記装置は、前記クライアントから入力された乱数を前記秘密鍵で暗号化し、記憶する機器識別子を前記共通鍵で暗号化し、前記暗号化された乱数及び前記暗号化された機器識別子を前記クライアントに出力する装置であることを特徴とする請求項８記載のデータ更新システム。

【請求項１０】　装置は、秘密鍵で暗号化された機器認証子をクライアントに出力する装置であり、

前記クライアントは、前記装置から入力された機器認証子をサーバに送信するクライアントであり、

前記サーバは、前記クライアントから受信した機器認証子を当該機器認証子に対応する公開鍵で復号して機器識別子を取得し、当該取得した機器識別子と記憶する機器識別子とを比較照合して機器認証を行うサーバであることを特徴とする請求項６又は７記載のデータ更新システム。

【請求項１１】　サーバとクライアント間の通信パケットが暗号化されることを特徴とする請求項８乃至１０の

いずれか記載のデータ更新システム。

【請求項１２】　装置は、発行元認証に用いる共通鍵又は公開鍵を記憶し、当該共通鍵又は公開鍵で暗号化された発行元認証子をクライアントに出力する装置であり、前記クライアントは、前記暗号化された発行元認証子をサーバに送信するクライアントであり、

前記サーバは、発行元認証に用いる共通鍵又は秘密鍵を記憶し、前記クライアントから受信した暗号化された発行元機器認証子を当該記憶する共通鍵又は秘密鍵で復号して発行元識別子を取得し、当該取得した発行元識別子と記憶する発行元識別子とを比較照合して発行元サーバ認証を行うサーバであることを特徴とする請求項８乃至１１のいずれかに記載のデータ更新システム。

【請求項１３】　クライアントは、発行元から発行元認証子を取得し、発行元サーバ認証の前に、装置から読み込んだ発行元認証子と前記取得した発行元認証子とを比較照合して発行元クライアント認証を行うクライアントであることを特徴とする請求項１２記載のデータ更新システム。

【請求項１４】　装置は、本人認証の機能を備え、クライアントでは発行元クライアント認証を、前記装置では本人認証を、サーバでは発行元サーバ認証、機器認証を、前記装置ではデータ更新を行うことを特徴とする請求項１３記載のデータ更新システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＩＣカード等に記憶されているデータを、ネットワークを介して新規登録や追加登録を含む更新を行うデータ更新方法に係り、特に、装置を間違いなく特定して更新することができ、確実、安全に人手を介さずに更新できるデータ更新方法及びデータ更新システムに関する。

【０００２】

【従来の技術】従来、ＩＣカード（スマートカード）その他取り外し可能な本人認証の機能を備えた装置に記憶された重要なデータ、例えば、ネットワークパスワード、電子証明書、シングルサインオンするための情報の追加、ダイヤルアップ情報、ＩＣカード／スマートカードや指紋照合トークン内情報、有効期限等の重要な情報を更新する場合には、当該ＩＣカードを一旦回収してデータの書き替えを行って本人に戻すか、そのカードを無効にして更新データが書き込まれた新規のカードを本人に発行するかのいずれかの方法が採用されている。

【０００３】尚、個人認証に用いる重要データを更新する技術ではないが、個人認証に関する従来技術には、平成１４年３月１２日公開の特開２００２－７３５７１「個人認証システムおよび個人認証方法、並びにプログラム提供媒体」（出願人：ソニー株式会社、発明者：渡辺秀明他）がある。この発明は、個人識別データであるテンプレートを格納した個人識別証明書を用いた個人認証システムにおける個人識別証明書の管理を行うものである。

【０００４】

【発明が解決しようとする課題】しかしながら、上記従来の取り外し可能な本人認証機能を備えた装置内部のデータ更新方法では、回収・再発行又は新規発行の手間が掛かり、重要データが外部に漏洩することなくネットワークを介して更新できず、利便性に欠けるという問題点があった。

【０００５】本発明は上記実情に鑑みて為されたものであり、装置を間違えなく特定し、ネットワークを介して記録媒体のデータを新規登録や追加登録を含む更新を自動で又は処理を起動して行うことができるデータ更新方法及びデータ更新システムを提供することを目的とする。

【０００６】

【課題を解決するための手段】本発明は、新規登録又は追加登録を含む更新を行うデータ更新方法において、機器認証に用いる秘密鍵を記憶する装置についてサーバが機器認証を行い、当該秘密鍵に対応する公開鍵を用いて暗号化された更新データを装置が接続するクライアントに送信し、当該クライアントが装置に当該更新データを入力し、装置が秘密鍵で更新データを復号し、復号した更新データで装置内のデータ更新を行うものであり、更新データを書き替える対象の装置を間違えることなく、機器認証に用いる秘密鍵を保有する装置のみが更新データを復号して更新でき、更新データの秘匿性を保持し、ネットワークを介して装置内のデータ更新を実現できる。

【０００７】本発明は、新規登録又は追加登録を含む更新を行うデータ更新方法において、機器認証に用いる秘密鍵を記憶する装置についてサーバが機器認証を行い、当該秘密鍵に対応する公開鍵を用いて暗号化された更新データを装置が接続するクライアントに送信し、当該クライアントが装置に当該更新データを入力し、装置が更新データを記憶し、更新データが利用される毎に秘密鍵で更新データを復号し、復号した更新データを利用のために提供するものであり、更新データの記憶先となる装置を間違えることなく、機器認証に用いる秘密鍵を保有する装置のみが更新データを復号して利用でき、更新データの秘匿性を保持し、ネットワークを介して装置内のデータ提供を実現できる。

【０００８】本発明は、データ更新システムにおいて、機器認証に用いる秘密鍵を記憶する装置と、機器認証が為されると、秘密鍵に対応する公開鍵で暗号化された更新データを機器認証が為された装置宛に送信するサーバと、送信された暗号化された更新データを受信して装置に出力するクライアントとを備え、装置は、クライアントから入力された暗号化された更新データを秘密鍵で復号し、当該復号した更新データで装置内のデータ更新を

行う装置としており、更新データを書き替える対象の装置を間違えることなく、機器認証に用いる秘密鍵を保有する装置のみが更新データを復号して更新でき、更新データの秘匿性を保持し、ネットワークを介して装置内のデータ更新を実現できる。

【０００９】本発明は、データ更新システムにおいて、機器認証に用いる秘密鍵を記憶する装置と、機器認証が為されると、秘密鍵に対応する公開鍵で暗号化された更新データを機器認証が為された装置宛に送信するサーバと、送信された暗号化された更新データを受信して装置に出力するクライアントとを備え、装置は、クライアントから入力された暗号化された更新データを記憶し、更新データが利用される毎に秘密鍵で更新データを復号し、当該復号した更新データを利用のために提供する装置としており、更新データの記憶先となる装置を間違えることなく、機器認証に用いる秘密鍵を保有する装置のみが更新データを復号して利用でき、更新データの秘匿性を保持し、ネットワークを介して装置内のデータ提供を実現できる。

【００１０】本発明は、上記データ更新方法又は上記データ更新システムにおいて、発行元クライアント認証、本人認証、発行元サーバ認証を行うものであり、セキュリティを向上させることができる。

【００１１】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら説明する。本発明の実施の形態に係るデータ更新システムは、本人認証、発行元認証、機器認証の各認証が為されると、機器認証子に対応する公開鍵で暗号化された更新データをサーバがクライアントに送信すると、ＩＣカードが当該暗号化された更新データをＩＣカード内の機器認証子に対応する秘密鍵で復号化し、その復号した更新データでＩＣカード内の書き替えを行うものである。これにより、ＩＣカードを回収することなく、重要データの秘匿性を保持しつつネットワークを介してＩＣカード内の重要データの更新（新規登録又は追加登録を含む）を自動で又は処理を起動して行うことができるものである。

【００１２】本発明の実施の形態に係るデータ更新システム（本システム）について図１を参照しながら説明する。図１は、本発明の実施の形態に係るデータ更新システムの概略構成図である。本システムは、図１に示すように、サーバ１と、ＤＢ（データベース）２と、インターネット３と、クライアント４と、ＩＣカードリーダライタ５と、ＩＣカード６と、発行元サーバ７と、ＩＣカードリーダライタ８とから基本的に構成されている。図１では、説明を簡単にするために、クライアント４，ＩＣカードリーダライタ５，ＩＣカード６は一台づつしか描画していないが、インターネット３に接続するクライアント４等は複数あるものである。また、クライアント４とサーバ１は、インターネット３を介して接続され、発行元サーバ７はサーバ１に接続している。

【００１３】次に、本システムの各部を具体的に説明する。サーバ１は、クライアント４からのインターネット３を介しての本処理（更新処理）に際して、本人認証処理、発行元認証処理、機器認証処理を行い、全て認証されると、ＤＢ２に記憶するクライアントに関するデータ（暗号データ）を、インターネット３を介してクライアント４に送信する。

【００１４】ここで、本人認証処理は、指紋データ、音声データ、顔の画像データ、又は孔彩、網膜、サイン、掌形の画像データ等の生体データ及び／又はＰＩＮ（Personal Identification Number）を用いた単独又は複合認証であり、ＩＣカード６とクライアント４との間で、若しくはＩＣカード６内で認証を行う。

【００１５】また、発行元認証処理は、クライアント４が保持する認証用のソフトウェア（インストーラによってインストールされたソフトウェア）の動作により、ＩＣカード６内の発行元認証子とクライアント４のメモリ内の発行元認証子とを比較照合して認証を行う発行元クライアント認証と、認証用のソフトウェアの動作により、ＩＣカード６内の発行元認証子をサーバ１に送信し、サーバ１で送信された発行元認証子を復号して発行元識別子を取得し、その発行元識別子とＤＢ２に記憶する発行元識別子とを比較照合して認証を行う発行元サーバ認証とを有する。インストーラは、発行元サーバ７からオンライン又はオフラインにてクライアント４に提供されるものである。

【００１６】特に、発行元サーバ認証を具体的に説明すると、ＩＣカード６の発行元が付与した発行元識別子とそれを共通鍵又は公開鍵（共通鍵／公開鍵）で暗号化した発行元認証子がＩＣカード６に記憶されており、その暗号化された発行元認証子がＩＣカード６からクライアント４を介してサーバ１に送信され、サーバ１で暗号化された発行元認証子を共通鍵又は秘密鍵（共通鍵／秘密鍵）で復号して発行元識別子を取り出し、ＤＢ２に記憶する発行元識別子と比較して復号した発行元識別子が適正であるか否かを判断する。ここで、発行元認証における暗号化及び復号化に用いる暗号鍵方式は、共通鍵方式又は公開鍵方式を用いている。特に、公開鍵方式の場合、公開鍵を保有するのはＩＣカード６側であり、それに対応する秘密鍵を保有するのはサーバ１である。また、サーバ１には、接続する発行元サーバ７からＩＣカード６に発行した発行元識別子と発行元認証子が予め提供されており、その発行元識別子と発行元認証子はＤＢ２に記憶される。

【００１７】更に、機器認証処理は、チャレンジレスポンス（オンライン認証）を用いた機器認証である。具体的には、サーバ１で乱数を発生させ、その乱数をクライアント４に送信する。クライアント４は、サーバ１から受信した乱数をＩＣカード６に出力し、ＩＣカード６は

保有する秘密鍵でその乱数を暗号化し、その暗号化した乱数及び保有する機器識別子をクライアント４に出力して、クライアント４が暗号化した乱数及び機器識別子をサーバ１に送信する。すると、サーバ１は、機器識別子から対応する公開鍵を取得し、暗号化された乱数をその公開鍵で復号化し、復号した乱数を発生させた乱数と比較照合し、一致すれば機器認証が成功したとする。

【００１８】また、サーバ１が、ＩＣカード６における機器識別子を暗号化するための共通鍵を乱数と共に送信してもよい。この場合、ＩＣカード６では、受信した共通鍵を用いて機器識別子を暗号化し、暗号化した乱数と暗号化した機器識別子をサーバ１に送信する。そして、サーバ１は、受信した暗号化された機器識別子を内部に保持する共通鍵で復号し、復号した機器識別子に対応する公開鍵を取得し、その公開鍵で暗号化された乱数を復号化して乱数の比較照合を行う。

【００１９】また、サーバ１とクライアント４との間における通信パケットをＳＳＬ（Secure Socket Layer）又はＶＰＮ（Virtual Private Network）等の技術を用いて暗号化してもよい。ＳＳＬ等の暗号化はサーバ１とクライアント４との間で有効であるが、クライアント４とＩＣカード６との間については、本処理が機密保護について有効である。

【００２０】尚、チャレンジレスポンスを用いない機器認証の場合には、ＩＣカード６が記憶する機器識別子を、記憶する秘密鍵で暗号化して機器認証子を生成し、クライアント４に出力する。クライアント４は、暗号化された機器認証子をサーバ１に送信し、サーバ１が暗号化された機器認証子に対応する公開鍵で復号して機器識別子を取得し、その機器識別子とＤＢ２に記憶する機器識別子と比較照合し、一致すれば機器認証が成功したものとしてもよい。

【００２１】また、サーバ１は、ＩＣカード６内の重要データを更新するための更新データを暗号化してＤＢ２に記憶している。その暗号方法は、機器識別子に対応する公開鍵を用いて暗号化している。そして、サーバ１は、ＩＣカード６内の重要データを更新するために、ＤＢ２に記憶する暗号化された更新データを、インターネット３を介してクライアント４に送信する。

【００２２】ＤＢ（データベース）２は、発行元認証を行うための発行元識別子、発行元認証子、共通鍵／秘密鍵、機器認証を行うための機器識別子、機器認証子、公開鍵、ＩＣカード６の重要データを更新するための暗号化された更新データを記憶している。ここで、発行元識別子を暗号化したのが発行元認証子で、乱数又は機器識別子を暗号化したのが機器認証子である。尚、サーバ１での認証処理では、復号された発行元識別子、機器識別子が取得されるので、ＤＢ２には、発行元認証のための発行元識別子、共通鍵／秘密鍵、機器認証のための機器識別子、公開鍵、更新データを最小限記憶していれば足りる。

【００２３】インターネット３は、サーバ１とクライアント４との間の通信媒体である。インターネット３の代わりにＷＡＮ（Wade Area Network）又はＬＡＮ（Local Area Network）等の通信媒体であってもよい。

【００２４】クライアント４は、本システムに接続するコンピュータであり、本人認証、発行元認証、機器認証等の認証により本システムにおける更新処理が許可され、サーバ１からの情報をＩＣカード６に書き込む。尚、クライアント４には発行元サーバ７がネットワークを介したオンラインで又はＣＤ－ＲＯＭ等の記録媒体を介したオフラインで発行されたインストーラによってインストールされた認証用のソフトウェアを保持しており、クライアントにおける発行元認証（発行元クライアント認証）を行うと共に、サーバ１にＩＣカード６内の発行元認証子を送信してサーバにおける発行元認証（発行元サーバ認証）を行う。

【００２５】具体的には、クライアント４は、認証用のソフトウェアを動作させ、発行元クライアント認証を行うために、ＩＣカード６からＩＣカードリーダライタ５で発行元認証子を読み込み、メモリに記憶する発行元認証子と比較照合し、一致すれば発行元クライアント認証が成功したものとして、次に発行元サーバ認証を行う。クライアント４は、発行元サーバ認証のために、ＩＣカード６からＩＣカードリーダライタ５で発行元認証子を読み取ってインターネット３を介してサーバ１に送信する。

【００２６】また、クライアント４は、機器認証のために、サーバ１から受信した乱数をＩＣカード６に出力し、ＩＣカード６において機器識別子に対応する秘密鍵でその乱数を暗号化して生成された機器認証子と、それに加えて機器識別子をＩＣカード６からＩＣカードリーダライタ５で読み取り、インターネット３を介してその機器認証子及び機器識別子をサーバ１に送信する。そして、各認証が為されると、データの更新処理として、クライアント４は、サーバ１から暗号化された更新データを受信し、そのデータをＩＣカード６に出力する。また、クライアント４は、ネットワークに接続可能なパーソナルコンピュータ（ＰＣ）、個人情報端末（ＰＤＡ）、携帯電話、ＰＨＳ、情報家電であってもよい。

【００２７】本人認証は、生体データ、ＰＩＮデータを単独又は複合的に用いて行われるもので、ＩＣカード６内又はＩＣカード６とクライアント４との間で認証される。また、暗号化された発行元認証子と機器認証子もＩＣカード６から読み込まれてクライアント４からサーバ１に送信される。ここで、本人認証で本人と認められない場合には、それに続く発行元認証、機器認証を行わない。

【００２８】ＩＣカードリーダライタ５は、ＩＣカード６内の情報を読み取ってクライアント４に出力し、ま

た、クライアント４からの指示によりＩＣカード６に情報を書き込む処理を行う。

【００２９】ＩＣカード６は、ＣＰＵ（Central Processing Unit）を備えて独立して処理を行うことができるものであり、本人認証を行う生体データ、ＰＩＮデータを、発行元認証を行うための発行元識別子、発行元認証子、共通鍵／公開鍵を、機器認証を行うための機器識別子、秘密鍵を記憶している。ここで、各データは、ＩＣカード６を無理にこじ開けた場合に、消滅する耐タンパー性を備えている。

【００３０】ＩＣカード６は、内部に保持する生体データ、ＰＩＮデータによって本人認証を行い、発行元クライアント認証においては発行元認証子をクライアント４に出力し、また、発行元サーバ認証においては発行元認証子をクライアント４に出力する。そして、チャレンジレスポンスによる機器認証の場合、ＩＣカード６は、サーバ１から送信された乱数をクライアント４から入力し、その乱数を秘密鍵で暗号化して機器認証子を生成し、生成した機器認証子と機器識別子をクライアント４に出力する。機器認証子及び機器識別子は、クライアント４からサーバ１に送信される。

【００３１】また、サーバ１から、ＩＣカード６における機器識別子を暗号化するための共通鍵を乱数と共に送信してもよい。この場合、ＩＣカード６は、受信した共通鍵を用いて機器識別子を暗号化し、暗号化した乱数と暗号化した機器識別子をサーバ１に送信する。そして、サーバ１は、受信した暗号化された機器識別子を内部に保持する共通鍵で復号し、復号した機器識別子に対応する公開鍵を取得し、その公開鍵で暗号化された乱数を復号化して乱数の比較照合を行う。これにより、暗号化されていない機器識別子がネットワークを流れることを防止できる。また、サーバ１とクライアント４との間における通信パケットをＳＳＬ又はＶＰＮ等の技術を用いて暗号化してもよい。

【００３２】また、チャレンジレスポンスによらない機器認証の場合、ＩＣカード６は、機器識別子を秘密鍵で暗号化して機器認証子を生成し、その機器認証子をクライアント４に出力する。

【００３３】尚、本システムでは、ＩＣカードを例に説明したが、トークン、独立型指紋認証装置（ＩＡＵ：Intelligent Authentication Unit）、その他取り外し可能な本人認証機能を備えた装置であってもよい。

【００３４】発行元サーバ７は、ＩＣカードリーダライタ８を備え、ＩＣカード６の発行元で決められた発行元認証のための発行元識別子、発行元認証子、共通鍵／公開鍵及びＩＣカード６の各々に対応した機器認証のための機器識別子、機器認証子、秘密鍵をＩＣカード６にオフラインで書き込むと共に、サーバ１に当該ＩＣカード６の発行元識別子、発行元認証子、共通鍵／秘密鍵と機器識別子、機器認証子、公開鍵をオンラインで送信し、ＤＢ２に発行元認証子、機器認証子等を記憶する。ここで、発行元識別子、発行元認証子は発行元にユニークな情報であり、機器識別子、機器認証子は機器にユニークな情報である。また、発行元サーバ７は、クライアント４の認証用のソフトウェアの動作によって発行元クライアント認証のための発行元認証子をクライアント４に登録する。

【００３５】発行元認証のためにＩＣカード６に書き込まれる共通鍵／公開鍵とＤＢ２に書き込まれる共通鍵／秘密鍵は対応しており、また、機器認証のためにＩＣカード６に書き込まれる秘密鍵とＤＢ２に書き込まれる公開鍵は対応しており、一方の鍵で暗号化されたデータを他方の鍵で復号できるものとなっている。尚、機器認証のためのＤＢ２に書き込まれる公開鍵は、ＩＣカード６で更新される更新データを暗号化するのに用いられ、機器認証のためのＩＣカード６に書き込まれる秘密鍵は、サーバ１から送信される暗号化された更新データを復号するのにも用いられる。

【００３６】尚、チャレンジレスポンスによる機器認証を行う場合は、ＩＣカード６に書き込む機器認証のための情報は、機器識別子と秘密鍵である。チャレンジレスポンスによらない機器認証を行う場合は、ＩＣカード６に書き込む機器認証のための情報は、機器識別子、機器認証子、秘密鍵である。ここで、機器認証の度に、機器識別子を秘密鍵で暗号化して機器認証子を生成してサーバ１に送信すれば、ＩＣカード６には機器識別子と秘密鍵が書き込まれればよい。

【００３７】次に、本システムの動作について図２、図３、図４を用いて説明する。図２は、本発明の実施の形態に係る新規登録又は追加登録を含む更新処理を行うデータ更新システムにおける処理の概要を示す処理概略図であり、図３は、サーバ１における処理の流れを示すフローチャートであり、図４は、ＩＣカード６における処理の流れを示すフローチャートである。

【００３８】図２に示すように、クライアント４は、認証用ソフトウェアが動作し、ＩＣカード６から発行元認証子を読み込み、クライアント４内の発行元認証子と比較照合して発行元クライアント認証（１）を行う。比較照合の結果、一致していれば発行元クライアント認証が成功したとして、次に、ユーザは生体データ又はＰＩＮデータ等を用いてＩＣカード６での本人認証（２）を行う。

【００３９】本人認証が適正であれば、次に、ＩＣカード６は、発行元認証子をクライアント４からサーバ１に送信してサーバ１での発行元サーバ認証（３）を行う（Ｓ１）。発行元サーバ認証は、ＩＣカード６から出力された発行元認証子をサーバ１が受信し、ＤＢ２に記憶する復号のための共通鍵／秘密鍵を用いて復号化し、復号された発行元識別子を取得して、ＤＢ２に記憶する発行元識別子と比較照合する。比較照合結果、一致すれば

発行元サーバ認証が成功したとして、次に機器認証（４）を行う。

【００４０】チャレンジレスポンスによる機器認証（４）（Ｓ２）は、サーバ１で乱数を発生させ、クライアント４を介してＩＣカード６にその乱数を送信する。ＩＣカード６では機器認証のための秘密鍵でその乱数を暗号化し、機器識別子（又はサーバ１から送信された共通鍵で暗号化された機器識別子）と暗号化された乱数をクライアント４を介してサーバ１に送信する。サーバ１は、機器識別子（暗号化された機器識別子であればサーバ１が保持する共通鍵で復号した機器識別子）に対応する公開鍵で暗号化された乱数を復号し、復号した乱数と当初発生させた乱数とを比較照合して、機器認証を行う。比較照合の結果、両者が一致すれば、機器認証は成功したものとなる。

【００４１】また、チャレンジレスポンスによらない機器認証の場合、ＩＣカード６は機器識別子を機器認証のための秘密鍵で暗号化して機器認証子を生成し、クライアント４を介してサーバ１に送信する。サーバ１は、機器認証子を受信し、その機器認証子に対応する公開鍵で機器認証子を復号して機器識別子を取得し、ＤＢ２に記憶する機器識別子と復号した機器識別子とを比較照合して、機器認証を行う。比較照合の結果、両者が一致すれば、機器認証は成功したものとなる。

【００４２】機器認証が適正に終了すると、サーバ１は、機器認証のための公開鍵で暗号化された更新データをＤＢ２から読み込み、クライアント４にインターネット３を介して転送し、クライアント４はその暗号化された更新データをＩＣカード６に出力する（５）（Ｓ３）。

【００４３】更に、ＩＣカード６は、暗号化された更新データを入力し（Ｓ１１）、当該更新データをＩＣカード内の機器認証のための秘密鍵で復号化する（Ｓ１２）（６）。そして、復号化された復号データでＩＣカード６内の重要なデータを書き替えて更新する（Ｓ１３）（７）。尚、ＩＣカード６は、入力した暗号化された更新データをそのままの状態で記憶し、当該更新データを参照する必要が発生した場合に秘密鍵で復号して利用するようにしてもよい。

【００４４】本システムによれば、本人認証、発行元認証、機器認証を行い、機器認証のための公開鍵で暗号化された更新データをサーバ１がＤＢ２から読み取ってクライアント４に送信し、クライアント４では受信した暗号化された更新データをＩＣカード６に出力し、ＩＣカード６は、機器認証のための秘密鍵で更新データを復号して、ＩＣカード６内のデータの書き替えを行うようにしているので、機器認証を行うことで更新データを書き替える対象のＩＣカードを間違えることがなく、更新データが盗聴されたとしても、機器認証のための秘密鍵を保有するＩＣカード６のみがデータを復号可能であるためセキュリティを向上させることができ、サーバ１は対象とするＩＣカード６内の重要なデータを、ネットワークを介して更新できる効果がある。

【００４５】また、本システムでは、ＩＣカード６内のデータ更新の処理について説明したが、ユーザが本システムのネットワークにログインする際に、本人認証、発行元認証、機器認証を行い、ユーザが意識した処理をすることなく、自動でシステム変更に伴うデータをＩＣカード６に書き込むことが可能となる。これにより、アプリケーションの有効期限、更新期限、電子証明書の有効期限の更新、ネットワークパスワードのユーザ毎の定期的変更等を容易に行うことができる効果がある。

【００４６】具体的には、ネットワークパスワードを定期的に変更する場合は、変更日にＤＢ２に変更されたパスワードを公開鍵で暗号化してセットし、ユーザログインにより、各認証が行われ、適正であればサーバ１がＤＢ２から暗号化されたパスワードをクライアント４に送信し、クライアント４が暗号化されたパスワードをＩＣカード６に出力する。ＩＣカード６は、入力された暗号化されたパスワードを秘密鍵で復号し、その復号したパスワードをＩＣカード６内に記憶する。これにより、ＩＣカード６におけるネットワークパスワードが変更されたことになる。

【００４７】

【発明の効果】本発明によれば、機器認証に用いる秘密鍵を記憶する装置についてサーバが機器認証を行い、当該秘密鍵に対応する公開鍵を用いて暗号化された更新データを装置が接続するクライアントに送信し、当該クライアントが装置に当該更新データを入力し、装置が秘密鍵で更新データを復号し、復号した更新データで装置内のデータ更新を行う、新規登録又は追加登録を含む更新を行うデータ更新方法としているので、更新データを書き替える対象の装置を間違えることなく、機器認証に用いる秘密鍵を保有する装置のみが更新データを復号して更新でき、更新データの秘匿性を保持し、ネットワークを介して装置内のデータ更新を実現できる効果がある。

【００４８】本発明によれば、機器認証に用いる秘密鍵を記憶する装置についてサーバが機器認証を行い、当該秘密鍵に対応する公開鍵を用いて暗号化された更新データを装置が接続するクライアントに送信し、当該クライアントが装置に当該更新データを入力し、装置が更新データを記憶し、更新データが利用される毎に秘密鍵で更新データを復号し、復号した更新データを利用のために提供する、新規登録又は追加登録を含む更新を行うデータ更新方法としているので、更新データの記憶先となる装置を間違えることなく、機器認証に用いる秘密鍵を保有する装置のみが更新データを復号して利用でき、更新データの秘匿性を保持し、ネットワークを介して装置内のデータ提供を実現できる効果がある。

【００４９】本発明によれば、機器認証に用いる秘密鍵

13

を記憶する装置と、機器認証が為されると、秘密鍵に対応する公開鍵で暗号化された更新データを機器認証が為された装置宛に送信するサーバと、送信された暗号化された更新データを受信して装置に出力するクライアントとを備え、装置は、クライアントから入力された暗号化された更新データを秘密鍵で復号し、当該復号した更新データで装置内のデータ更新を行うデータ更新システムとしているので、更新データを書き替える対象の装置を間違えることなく、機器認証に用いる秘密鍵を保有する装置のみが更新データを復号して更新でき、更新データの秘匿性を保持し、ネットワークを介して装置内のデータ更新を実現できる効果がある。

【００５０】本発明によれば、機器認証に用いる秘密鍵を記憶する装置と、機器認証が為されると、秘密鍵に対応する公開鍵で暗号化された更新データを機器認証が為された装置宛に送信するサーバと、送信された暗号化された更新データを受信して装置に出力するクライアントとを備え、装置は、クライアントから入力された暗号化された更新データを記憶し、更新データが利用される毎に秘密鍵で更新データを復号し、当該復号した更新データを利用のために提供するデータ更新システムとしているので、更新データの記憶先となる装置を間違えることなく、機器認証に用いる秘密鍵を保有する装置のみが更＊

14

＊新データを復号して利用でき、更新データの秘匿性を保持し、ネットワークを介して装置内のデータ提供を実現できる効果がある。

【００５１】本発明によれば、発行元クライアント認証、本人認証、発行元サーバ認証を行う上記データ更新方法又は上記データ更新システムとしているので、セキュリティを向上させることができる効果がある。

【図面の簡単な説明】

【図１】本発明の実施の形態に係るデータ更新システムの概略構成図である。

【図２】本発明の実施の形態に係る新規登録又は追加登録を含む更新処理を行うデータ更新システムにおける処理の概要を示す処理概略図である。

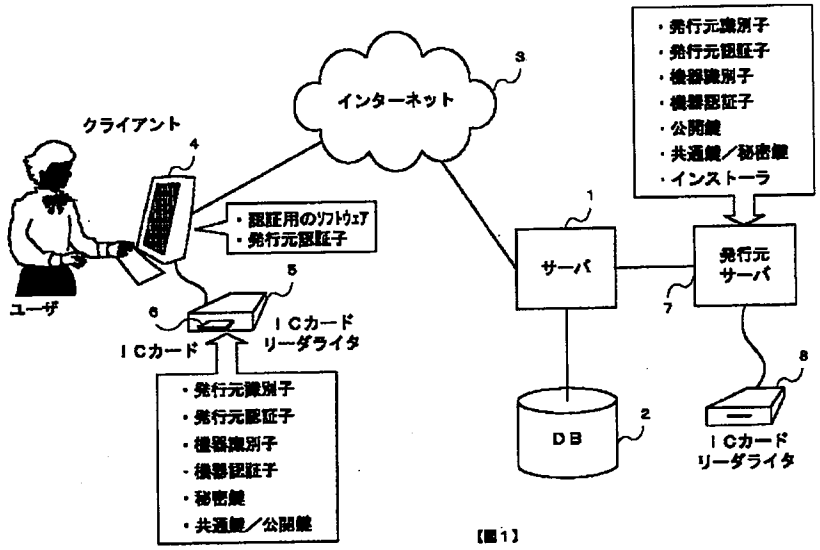
【図３】サーバ１における処理の流れを示すフローチャートである。

【図４】ＩＣカード６における処理の流れを示すフローチャートである。

【符号の説明】

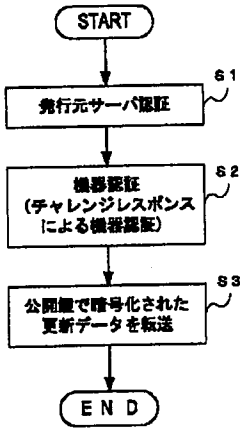
１…サーバ、　２…ＤＢ、　３…インターネット、　４…クライアント、　５…ＩＣカードリーダライタ、　６…ＩＣカード、　７…発行元サーバ、　８…ＩＣカードリーダライタ

【図１】



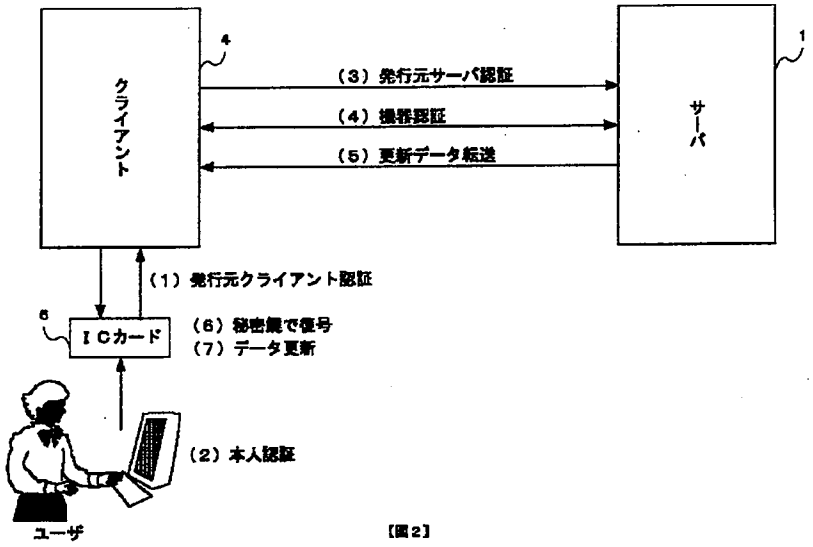
【図１】

【図３】



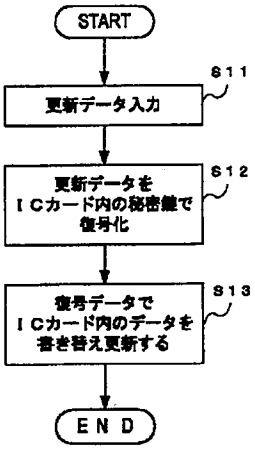
【図３】

【図２】



【図２】

【図４】



【図４】

【手続補正書】
【提出日】平成１５年４月７日（２００３．４．７）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】請求項３
【補正方法】変更
【補正内容】
【請求項３】　機器認証に用いる秘密鍵を記憶する装置には、共通鍵又は公開鍵で暗号化された発行元認証子が記憶され、サーバは前記共通鍵又は前記公開鍵に対応する秘密鍵を用い、前記装置からの暗号化された発行元認証子を当該共通鍵又は当該秘密鍵で復号して発行元識別子を取得し、当該取得した発行元識別子と記憶する発行元識別子とを比較照合して発行元サーバ認証を行うことを特徴とする請求項１又は２記載のデータ更新方法。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】請求項８
【補正方法】変更
【補正内容】
【請求項８】　サーバは、乱数を発生させ、当該乱数をクライアントに送信すると共に、前記クライアントから受信した暗号化された乱数を受信した機器識別子に対応する公開鍵で復号し、当該復号された乱数と前記発生させた乱数を比較照合して機器認証を行うサーバであり、
前記クライアントは、前記サーバから受信した乱数を装置に出力すると共に、前記装置から入力された暗号化された乱数及び機器識別子を前記サーバに送信するクライアントであり、
前記装置は、前記クライアントから入力された乱数を、記憶する秘密鍵で暗号化し、記憶する機器識別子と前記暗号化された乱数を前記クライアントに出力する装置であることを特徴とする請求項６又は７記載のデータ更新システム。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】請求項９
【補正方法】変更
【補正内容】
【請求項９】　サーバは、乱数と、機器識別子を暗号化するための共通鍵をクライアントに送信し、前記クライアントから受信した暗号化された機器識別子を前記共通鍵で復号し、当該復号された機器識別子に対応する公開鍵で暗号化された乱数を復号し、当該復号された乱数と前記発生させた乱数を比較照合して機器認証を行うサーバであり、
前記クライアントは、前記サーバから受信した乱数及び共通鍵を装置に出力すると共に、前記装置から入力された暗号化された乱数及び暗号化された機器識別子を前記サーバに送信するクライアントであり、
前記装置は、前記クライアントから入力された乱数を、記憶する秘密鍵で暗号化し、記憶する機器識別子を前記共通鍵で暗号化し、前記暗号化された乱数及び前記暗号化された機器識別子を前記クライアントに出力する装置であることを特徴とする請求項８記載のデータ更新システム。
【手続補正４】

【補正対象書類名】明細書
【補正対象項目名】請求項１２
【補正方法】変更
【補正内容】
【請求項１２】　装置は、発行元認証に用いる共通鍵又は公開鍵を記憶し、当該共通鍵又は公開鍵で暗号化された発行元認証子をクライアントに出力する装置であり、前記クライアントは、前記暗号化された発行元認証子をサーバに送信するクライアントであり、
前記サーバは、発行元認証に用いる共通鍵又は秘密鍵を記憶し、前記クライアントから受信した暗号化された発行元認証子を当該記憶する共通鍵又は秘密鍵で復号して発行元識別子を取得し、当該取得した発行元識別子と記憶する発行元識別子とを比較照合して発行元サーバ認証を行うサーバであることを特徴とする請求項８乃至１１のいずれかに記載のデータ更新システム。
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】０００２
【補正方法】変更
【補正内容】
【０００２】
【従来の技術】従来、ＩＣカード（スマートカード）や、その他取り外し可能な本人認証の機能を備えた装置に記憶された重要なデータ、例えば、ネットワークパスワード、電子証明書、シングルサインオンするための情報を追加する場合や、ダイヤルアップ情報、ＩＣカード／スマートカードや指紋照合トークン内情報、有効期限等の重要な情報を更新する場合には、当該ＩＣカードを一旦回収してデータの書き替えを行って本人に戻すか、そのカードを無効にして更新データが書き込まれた新規のカードを本人に発行するかのいずれかの方法が採用されている。
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】０００５
【補正方法】変更
【補正内容】
【０００５】本発明は上記実情に鑑みて為されたものであり、装置を間違えなく特定し、ネットワークを介して記録媒体のデータの新規登録や追加登録を含む更新を自動で又は処理を起動して行うことができるデータ更新方法及びデータ更新システムを提供することを目的とする。
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００１１
【補正方法】変更
【補正内容】
【００１１】
【発明の実施の形態】本発明の実施の形態について図面を参照しながら説明する。本発明の実施の形態に係るデータ更新システムは、本人認証、発行元認証、機器認証の各認証が為され、機器認証子に対応する公開鍵で暗号化された更新データをサーバがクライアントに送信すると、ＩＣカードが当該暗号化された更新データをＩＣカード内の機器認証子に対応する秘密鍵で復号化し、その復号した更新データでＩＣカード内の書き替えを行うものである。これにより、ＩＣカードを回収することなく、重要データの秘匿性を保持しつつネットワークを介してＩＣカード内の重要データの更新（新規登録又は追加登録を含む）を自動で又は処理を起動して行うことができるものである。
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００２９
【補正方法】変更
【補正内容】
【００２９】ＩＣカード６は、ＣＰＵ（Central Processing Unit）を備えて独立して処理を行うことができるものであり、本人認証を行う生体データ、ＰＩＮデータと、発行元認証を行うための発行元識別子、発行元認証子、共通鍵／公開鍵と、機器認証を行うための機器識別子、秘密鍵とを記憶している。ここで、各データは、ＩＣカード６を無理にこじ開けた場合に、消滅する耐タンパー性を備えている。
【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００３９
【補正方法】変更
【補正内容】
【００３９】本人認証が適正であれば、次に、ＩＣカード６は、発行元認証子をクライアント４からサーバ１に送信してサーバ１での発行元サーバ認証（３）を行う（Ｓ１）。発行元サーバ認証は、ＩＣカード６から出力された発行元認証子をサーバ１が受信し、ＤＢ２に記憶する復号のための共通鍵／秘密鍵を用いて復号化し、復号された発行元識別子を取得して、ＤＢ２に記憶する発行元識別子と比較照合する。比較照合の結果、一致すれば発行元サーバ認証が成功したとして、次に機器認証（４）を行う。